NRESTRAINT, TERMINATED,

U.S. District Court
District of Oregon (Portland (3))
CRIMINAL DOCKET FOR CASE #: 3:21−mj−00223−1

Case title: USA v. Sharp

Other court case number: 21−cr−714 Southern District of New York

Date Filed: 11/30/2021

Assigned to: Unassigned

Defendant (1)

Nickolas Sharp

represented by **Ryan Costello**
Federal Public Defender
101 SW Main Street
Suite 1700
Portland, OR 97204
503−326−2123
Fax: 503−326−5524
Email: ryan_costello@fd.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Public Defender or Community Defender Appointment

Pending Counts

None

Disposition

Highest Offense Level (Opening)

None

Terminated Counts

None

Disposition

Highest Offense Level (Terminated)

None

Complaints

18:1030(a)(5)(A)
TRANSMITTING A PROGRAM
TO A PROTECTED COMPUTER
WHICH INTENTIONALLY
CAUSED DAMAGE; 18:875(d)

Disposition

TRANSMITTING INTERSTATE
EXTORTION THREAT; 18:1343
WIRE FRAUD; 18:1001 FALSE
STATEMENTS

Plaintiff

USA	represented by	**Meredith Bateman**
		United States Attorney's Office
		1000 SW 3rd Avenue
		Ste #600
		Portland, OR 97204
		503–727–1087
		Email: meredith.bateman@usdoj.gov
		LEAD ATTORNEY
		ATTORNEY TO BE NOTICED
		Designation: Retained

Email All Attorneys

Date Filed	#	Page	Docket Text
11/30/2021	1		**(DOCUMENT FILED UNDER SEAL)**, Documents Received From Other Court as to Nickolas Sharp from Southern District of New York Case No: 21–cr–714 Initial Appearance is set for 12/1/2021 at 01:30PM in Portland by videoconference before Magistrate Judge John V. Acosta. (schm) (Entered: 12/01/2021)
11/30/2021	2		Documents Received Indictment From Other Court as to Nickolas Sharp from Southern District of New York Case No: 21–cr–714 (schm) (Entered: 12/01/2021)
12/01/2021	3		ORDER Granting Government's Oral Motion to unseal the case as to Nickolas Sharp (1). The Clerk is directed to unseal this case. Ordered by Magistrate Judge John V. Acosta. (pjg) (Entered: 12/01/2021)
12/01/2021	4		**Minutes of Proceedings:** Initial Appearance pursuant to Rule 5(c)(3) for Arrest in Our District Offense in Another. Proceedings before Magistrate Judge John V. Acosta as to Nickolas Sharp. Defendant waived an in–person appearance and consented to appear by video from USM Lockup. Defendant waived preliminary/identity hearing. Defendant advised of rights and waived reading of the charges. Order Appointing Counsel: Attorney Ryan Costello is appointed to represent Defendant for today's purposes. Defendant has hired private counsel for other proceedings. ORDER – Defendant is released on conditions. (See separate order.) Conditions of notification to employer and monitoring of employer's devices are STAYED. Defendant and retained counsel are to confer regarding these conditions and are to notify this Court of their position on these issues no later than noon on Monday, December 6, 2021. Other Court Information: USA v. Nickolas Sharp, 21 CRIM 714. Counsel Present for Government: Meredith Bateman. Counsel Present for Defendant: Ryan Costello. (Court Reporter: Jill Jessup) (pjg) (Entered: 12/01/2021)
12/01/2021	5		**Order Setting Conditions of Release** as to Defendant Nickolas Sharp. Signed

			on 12/1/2021 by Magistrate Judge John V. Acosta. (prvi). (Main Document 5 replaced on 12/1/2021, to remove unrelated page from PDF) (cw). Modified on 12/1/2021 (cw). (Entered: 12/01/2021)
12/01/2021	6		Waiver of Preliminary Examination or Hearing pursuant to Rule 5(c)(3) by Nickolas Sharp (schm) (Entered: 12/01/2021)
12/01/2021	7		Order Requiring Defendant to Appear in the Southern District of New York Where Charges are Pending and Transferring Bail as to Nickolas Sharp (schm) (Entered: 12/01/2021)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-- X
                                            :
UNITED STATES OF AMERICA
                                            :   **SEALED**
                                                 INDICTMENT
                                            :
          - v. -   21 Cr.
                                            :
NICKOLAS SHARP,   **2 1 CRIM 7 1 4**
                                            :
          Defendant.
                                            :
-- X
                                            :

                       COUNT ONE
   (Computer Fraud and Abuse – Intentionally Damaging Protected
                        Computers)

     The Grand Jury charges:

               Relevant Persons and Entities

     1.   At all times relevant to this Indictment, Company-1
was a technology company headquartered in New York, New York,
which manufactured and sold wireless communications products.
Company-1's shares are traded on the New York Stock Exchange.

     2.   At all times relevant to this Indictment, NICKOLAS
SHARP, the defendant, was a senior software engineer at
Company-1, responsible for software development and cloud
infrastructure security, among other things.

               Overview of the Criminal Scheme

     3.   From at least in or about 2020, up to and including
in or about 2021, NICKOLAS SHARP, the defendant, repeatedly

misused administrative access provided to him as an
information technology employee to download gigabytes of
Company-1's confidential data. During the course of this
cybersecurity incident (the "Incident"), SHARP caused damage
to Company-1's computer systems by altering log retention
policies and other files, to conceal his unauthorized activity
on the network. While working on a team remediating the
effects of the Incident, SHARP sent a ransom note to Company-
1, posing as an anonymous attacker who claimed to have
obtained unauthorized access to Company-1's computer networks.
The ransom note sought 50 Bitcoin, a cryptocurrency, which is
the equivalent of approximately $1.9 million based on the
prevailing exchange rate at the time, in exchange for the
return of the stolen data and the identification of an
existing "backdoor," or vulnerability to Company-1's computer
systems. After Company-1 refused the demand, SHARP published
a portion of the stolen files on a publicly accessible online
platform. SHARP subsequently engaged in a media campaign to
malign Company-1's response and disclosures related to the
Incident, while concealing his own role, causing Company-1 to
lose billions of dollars in market capitalization value.

2

Background

4.   At all times relevant to this Indictment, Company-1
used multiple third-party providers to host its data and
facilitate its product development. Company-1 maintained an
account with Amazon Web Services ("AWS"), which was used to
host server infrastructure and manage development of Company-
1's new applications and products. The AWS infrastructure
included servers that ran a portion of Company-1's operations
and hosted certain of Company-1's system, code, and
credentials.

5.   At all times relevant to this Indictment, Company-1
also subscribed to services from a third-party company named
GitHub, Inc. ("GitHub"), which is a provider of internet
hosting for software development, developer collaboration, and
version control. Through GitHub, Company-1 stored certain
development files, as well as the history of changes to those
files, in data structures called repositories. Developers
employed by Company-1 had individualized accounts on GitHub
which provided them with varying levels of access to various
repositories hosting Company-1's code and development
projects. Company-1 also maintained a high-level access
account shared among a group of developers ("GitHub Account-

3

1"), which provided access to all or nearly all of Company-1's repositories on GitHub. User activity on GitHub is logged.

6.   Keybase is an encrypted social networking service that permits users to, among other things, send private messages and files directly to other Keybase users and also to upload files that would be publicly available to any Keybase user.

7.   A Virtual Private Network ("VPN") is an internet connection method used to add security and privacy to network connections. When a user connects to a VPN, it creates an encrypted tunnel between the user and a remote server operated by a VPN service. All of the user's internet traffic is encrypted and routed through this tunnel to the ultimate internet or web resource being accessed by the user. Because internet traffic exits the VPN server, the user's computer appears to have the IP address of said server, masking the IP address of the user's computer, and thus his identity and location.

8.   Surfshark is a company headquartered in the British Virgin Islands that sells a commercial VPN service (the "Surfshark VPN") to the public, which, as described above, can effectively anonymize their users by replacing their personal

4

IP addresses with IP addresses operated by Surfshark through its servers.

The Cybersecurity Incident

9.   NICKOLAS SHARP, the defendant, was employed by Company-1 from in or about August 2018 up to and including on or about April 1, 2021, including throughout the time period of the Incident in or about December 2020, and the ransom demand in January 2021. SHARP was a senior developer who had access to credentials for Company-1's GitHub and AWS servers.

10.   On or about July 7, 2020, NICKOLAS SHARP, the defendant, used his personal Paypal, Inc. account to purchase a 27-month subscription to Surfshark VPN. SHARP downloaded Surfshark VPN on multiple devices, including his cell phone and laptop, and used the VPN service prior to the Incident.

11.   At all times relevant to this Indictment, NICKOLAS SHARP, the defendant, resided at a residence in Portland, Oregon (the "Sharp Residence"). The internet connection from the Sharp Residence was associated with a specific Internet Protocol address at certain relevant times (the "Sharp IP").

12.   On or about December 9, 2020, NICKOLAS SHARP, the defendant, applied for a position at a technology company based in California ("Company-2").

5

13.   On or about December 10, 2020, at approximately 2:55 a.m. UTC,[1] and again at 3:16 a.m., NICKOLAS SHARP, the defendant, used his own Company-1 credentials to access a particular key (the "Key") on Company-1's infrastructure through AWS servers. The connection was made through the Sharp IP. The Key accessed by SHARP permitted the user to, among other things, obtain access to other credentials within Company-1's infrastructure and to run searches through that infrastructure.

14.   Approximately two minutes later, on December 10, 2020, at approximately 3:18 a.m., an attacker connected to Company-1's AWS infrastructure using a masked IP provided by the Surfshark VPN. The attacker used the same Key accessed by NICKOLAS SHARP, the defendant, two minutes earlier to connect to AWS and to run a command "getcalleridentity." That command returns the username and account information for the AWS account for which it is run and can validate that the credential is usable.

15.   On December 21, 2020, at approximately 9:58 p.m., NICKOLAS SHARP, the defendant, logged into Company-1's GitHub infrastructure via a web browser, using his own Company-1 work

---

[1] For consistency, unless otherwise noted, all times are in the UTC time zone.

credentials. SHARP logged in through his Sharp IP address, and viewed the names of certain repositories of data.

16. Approximately one minute later, on December 21, 2020, at approximately 9:59 p.m., NICKOLAS SHARP, the defendant, used the Surfshark VPN that masked his true IP address to connect into GitHub through SSH by using Company-1's high-level GitHub Account-1.[2] SHARP used the SSH connection to execute a series of commands to clone Company-1's repositories of data to SHARP's computer.

17. Although throughout the vast majority of the Incident, NICKOLAS SHARP, the defendant, successfully masked his true IP address through the Surfshark VPN, in one fleeting instance during the exfiltration of data, the SHARP IP address was logged making an SSH connection to use GitHub Account-1 to clone a repository. Between December 21, 2020 at approximately 11:47 p.m. and December 22, 2020 at approximately 2:16 a.m., SHARP used the Surfshark VPN to mask his connection while cloning Company-1's GitHub repositories.

---

[2] SSH is a network protocol that gives users, such as system administrators, a way to access a remote machine. An SSH connection by itself does not reveal a list of available GitHub repositories, so a user intending to access or copy any particular repository would have needed to have acquired the names of those repositories through some other prior means, such as through a web browser connection described in the preceding paragraph.

7

No further clone commands were processed until approximately 39 minutes later, on December 22, 2020, at approximately 2:55 a.m., when GitHub Account-1 received a command to clone another repository from the Sharp IP associated with the Sharp Residence. Approximately nine minutes later, the clone commands continued from GitHub Account-1, once again masked by the Surfshark VPN.

18. On December 22, 2020 at approximately 2:16 a.m., the attacker's exfiltration commands stopped. At around the same time, the internet service at the Sharp Residence went down. At approximately 2:54 a.m., the Internet service at the Sharp Residence was reenabled, and approximately one minute later, the Sharp IP was logged, unmasked by any VPN, using GitHub Account-1 to continue sending clone commands.

19. Over the next several hours, on December 22, 2020 between approximately 3:04 to 5:31 a.m., NICKOLAS SHARP, the defendant, cloned approximately 155 repositories from Company-1 through GitHub Account-1, using the Surfshark VPN to once again mask his IP address.

20. NICKOLAS SHARP, the defendant, accessed Company-1's GitHub or AWS data using the Surfshark VPN through at least on or about December 26, 2020. Among other things, SHARP applied one-day lifecycle retention policies to certain logs on AWS

8

which would have the effect of deleting certain evidence of the intruder's activity within one day.

21. The Incident was discovered by other employees of Company-1 on or about December 28, 2020. At that time, NICKOLAS SHARP, the defendant, joined a team working to assess the scope and damage caused by the Incident and remediate its effects, all while concealing his role in committing the Incident. SHARP made numerous false statements to Company-1's employees and agents to evade detection. For example, upon the team's identification of Surfshark VPN as the tool used by the attacker, SHARP pretended to have never used Surfshark VPN himself.

22. On or about January 7, 2021, at approximately 4:01 a.m., senior employees at Company-1, including an employee located in Manhattan, New York, received a ransom email (the "Ransom Email") from the perpetrator of the Incident. The email was sent through an IP address associated with the Surfshark VPN. The Ransom Email offered, in substance, to return the stolen data and not to publish or use it, in exchange for the payment of 25 Bitcoin. The Ransom Email also offered to identify a purportedly still unblocked "backdoor" used by the attacker for the sum of another 25 Bitcoin. The total amount requested for ransom was equivalent to close to

9

$1.9 million, based on the prevailing exchange rate between
Bitcoin and U.S. dollars at the close of January 7, 2021. The
Ransom Email also referenced a chat communication on Keybase,
sent by the attacker to a senior security employee at Company-
1. That Keybase communication contained a copy of the Ransom
Email text as well as uploaded examples of Company-1's stolen
data.

23. Company-1 did not pay the ransom prior to the ransom
deadline set forth the Ransom Email. On or about January 9,
2021, at approximately 11:57 p.m., three minutes before the
ransom deadline was to expire, NICKOLAS SHARP, the defendant,
sent an employee of Company-1 a message on Keybase, as the
anonymous perpetrator of the Incident. The message read "No
BTC. No talk. We done here." The message contained a link to
a public Keybase folder on which the perpetrator had uploaded
certain of Company-1's stolen proprietary data for public
access. Company-1 promptly caused Keybase to remove the
folder.

24. On or about January 29, 2021, NICKOLAS SHARP, the
defendant, wiped and reset the laptop computer he used to
perpetrate the Incident.

25. On or about March 24, 2021, agents from the Federal
Bureau of Investigation ("FBI") executed a search warrant on

10

the Sharp Residence and seized certain electronic devices

belonging to NICKOLAS SHARP, the defendant. In the course of

the execution of that search, SHARP made numerous false

statements to FBI agents, including among other things, in

substance, that he was not the perpetrator of the Incident and

that he had not used Surfshark VPN prior to the discovery of

the Incident. When confronted with records demonstrating that

SHARP bought the Surfshark VPN service in July 2020,

approximately six months prior to the Incident, SHARP falsely

stated, in part and substance, that someone else must have

used his Paypal account to make the purchase.

26. Several days after the FBI executed a search warrant

on the SHARP Residence and seized certain electronic devices

belonging to NICKOLAS SHARP, the defendant, SHARP caused false

or misleading news stories to be published about the Incident

and Company-1's disclosures and response to the Incident.

SHARP identified himself as an anonymous source within

Company-1 who had worked on remediating the Incident. In

particular, SHARP pretended that Company-1 had been hacked by

an unidentified perpetrator who maliciously acquired root

administrator access Company-1's AWS accounts. In fact, as

SHARP well knew, SHARP had taken Company-1's data using

credentials to which he had access in his role as Company-1's

11

AWS cloud administrator, and SHARP had used that data in a
failed attempt to extort Company-1 for millions of dollars.

27. Following the publication of these articles, between
Tuesday, March 30, 2021 and Wednesday March 31, 2021, Company-
1's stock price fell approximately 20%, losing over four
billion dollars in market capitalization.

28. As a result of perpetrating the Incident, NICKOLAS
SHARP, the defendant, caused far in excess of $5,000 in losses
to Company-1, which included costs incurred by Company-1 to
retain forensic outside experts to investigate the Incident
and remediate the harm caused by SHARP.

Statutory Allegations

29. From at least in or about 2020, up to at least in or
about January 2021, in the Southern District of New York and
elsewhere, NICKOLAS SHARP, the defendant, knowingly caused the
transmission of a program, information, code, and command, and
as a result of such conduct, intentionally caused damage,
without authorization, to a protected computer, which caused a
loss aggregating to at least $5,000 in value to one and more
persons during any one-year period, to wit, SHARP, without
authorization, transmitted commands to servers to alter its
data retention policies in order to conceal SHARP's access, in

12

furtherance of a scheme to extort Company-1 for ransom to return its confidential data.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(c)(4)(A)(i)(I) and 2.)

COUNT TWO
(Transmission of Interstate Communications with Intent to Extort)

The Grand Jury further charges:

30.   The allegations in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

31.   From at least in or about 2020, up to at least in or about January 2021, in the Southern District of New York and elsewhere, NICKOLAS SHARP, the defendant, knowingly, and with intent to extort from a person, firm, association and corporation, any money and other thing of value, transmitted in interstate and foreign commerce a communication containing a threat to injure the property and reputation of the addressee and of another, to wit, SHARP transmitted an interstate email and other electronic messages to Company-1 seeking a ransom of 50 Bitcoin in exchange for returning data previously stolen by SHARP from Company-1, and to refrain from publicly identifying a purported remaining vulnerability to obtain unauthorized access to Company-1's computer systems.

13

(Title 18, United States Code, Sections 875(d) and 2.)

COUNT THREE
(Wire Fraud)

The Grand Jury further charges:

32. The allegations in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

33. From at least in or about 2020 to at least in or about April 2021, in the Southern District of New York and elsewhere, NICKOLAS SHARP, the defendant, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, SHARP, without authorization, downloaded confidential data belonging to Company-1 and altered retention policies to conceal his access, and then while representing that he was remediating the attack, anonymously extorted Company-1 for 50 Bitcoin to return the stolen data and identify a purported remaining vulnerability to obtain unauthorized access to

14

Company-1's computer systems, which involved interstate
communications into and out of the Southern District of New
York.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FOUR
(Making False Statements)

The Grand Jury further charges:

34. The allegations contained in paragraphs 1 through 28
of this Indictment are repeated and realleged as if fully set
forth herein.

35. In or about March, 2020, NICKOLAS SHARP, the
defendant, in a matter within the jurisdiction of the
executive branch of the Government of the United States,
knowingly and willfully made a materially false, fictitious,
and fraudulent statement and representation and made and used
a false writing and document knowing the same to contain a
materially false, fictitious, and fraudulent statement and
entry, to wit, SHARP made false statements to the FBI
regarding, among other things, SHARP's involvement in a
cybersecurity incident and extortion attempt at Company-1 in
December 2020 and January 2021, as well as SHARP's use of

15

Surfshark VPN, a particular tool employed by the perpetrator
of the incident.

(Title 18, United States Code, Sections 1001 and 2.)

FORFEITURE ALLEGATIONS

36. As a result of committing the offense alleged in
Count One of this Indictment, NICKOLAS SHARP, the defendant,
shall forfeit to the United States, pursuant to Title 18,
United States Code, Section 1030(i), any and all property,
real or personal, constituting or derived from, any proceeds
obtained directly or indirectly, as a result of said offenses,
and any and all personal property that was used or intended to
be used to commit or to facilitate the commission of said
offense, including but not limited to a sum of money in United
States currency representing the amount of proceeds traceable
to the commission of said offense.

37. As a result of committing the offenses alleged in
Counts Two and Three of this Indictment, NICKOLAS SHARP, the
defendant, shall forfeit to the United States, pursuant to
Title 18, United States Code, Section 981(a)(1)(C) and Title
28, United States Code, Section 2461(c), any and all property,
real and personal, that constitutes or is derived, directly or
indirectly, from proceeds traceable to the commission of said

16

offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

<u>Substitute Asset Provision</u>

38. If any of the above-described forfeitable property, as a result of any act or omission of NICKOLAS SHARP, the defendant:

      (a) cannot be located upon the exercise of due diligence;

      (b) has been transferred or sold to, or deposited with, a third person;

      (c) has been placed beyond the jurisdiction of the Court;

      (d) has been substantially diminished in value; or

      (e) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

    (Title 18, United States Code, Sections 1030 and 981;
        Title 21, United States Code, Section 853; and

17

Title 28, United States Code, Section 2461.)

_____
FOREPERSON

Damian Williams / kg

DAMIAN WILLIAMS
United States Attorney

18

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

NICKOLAS SHARP,

Defendant.

SEALED INDICTMENT

21 Cr. _____

(18 U.S.C. §§ 2, 875, 1001, 1030, and 1343.)

DAMIAN WILLIAMS
United States Attorney.

A TRUE BILL

████████████████████

FOREPERSON

Sealed Indictment, Arrest Warrant
filed 11/8/21 before CTW

```
MIME-Version:1.0
From:info@ord.uscourts.gov
To:nobody
Bcc:
--Case Participants:
--Non Case Participants:
--No Notice Sent:

Message-Id:7656129@ord.uscourts.gov
Subject:Activity in Case 21-223 Sealed v. Sealed (Redacted Notice)
```
Content–Type: text/html

U.S. District Court

District of Oregon

Notice of Electronic Filing

The following transaction was entered on 12/1/2021 at 1:33 PM PST and filed on 12/1/2021

Case Name:	USA v. SEALED
Case Number:	3:21–mj–00223 *SEALED*
Filer:	
Document Number:	3(No document attached)

Docket Text:
 ORDER Granting Government's Oral Motion to unseal the case as to Nickolas Sharp (1). The Clerk is directed to unseal this case. Ordered by Magistrate Judge John V. Acosta. (pjg)

3:21–mj–00223 *SEALED*–1 No electronic public notice will be sent because the case/entry is sealed.

```
MIME-Version:1.0
From:info@ord.uscourts.gov
To:nobody
Bcc:
--Case Participants: Ryan Costello (michelle_rawson@fd.org, orx_docketing@fd.org,
ryan_costello@fd.org)
--Non Case Participants: U.S. Marshal Service (pdx.operations@usdoj.gov), U.S. Pretrial
Services (cmecf@orpt.uscourts.gov)
--No Notice Sent:

Message-Id:7656207@ord.uscourts.gov
Subject:Activity in Case 3:21-mj-00223 USA v. Sharp Initial Appearance – Out of District
Warrant
```
Content–Type: text/html

U.S. District Court

District of Oregon

Notice of Electronic Filing

The following transaction was entered on 12/1/2021 at 2:13 PM PST and filed on 12/1/2021

Case Name:	USA v. Sharp
Case Number:	3:21–mj–00223
Filer:	
Document Number:	4(No document attached)

Docket Text:
Minutes of Proceedings: Initial Appearance pursuant to Rule 5(c)(3) for Arrest in Our District Offense in Another. Proceedings before Magistrate Judge John V. Acosta as to Nickolas Sharp. Defendant waived an in–person appearance and consented to appear by video from USM Lockup. Defendant waived preliminary/identity hearing. Defendant advised of rights and waived reading of the charges. Order Appointing Counsel: Attorney Ryan Costello is appointed to represent Defendant for today's purposes. Defendant has hired private counsel for other proceedings. ORDER – Defendant is released on conditions. (See separate order.) Conditions of notification to employer and monitoring of employer's devices are STAYED. Defendant and retained counsel are to confer regarding these conditions and are to notify this Court of their position on these issues no later than noon on Monday, December 6, 2021. Other Court Information: USA v. Nickolas Sharp, 21 CRIM 714. Counsel Present for Government: Meredith Bateman. Counsel Present for Defendant: Ryan Costello. (Court Reporter: Jill Jessup) (pjg)

3:21–mj–00223–1 Notice has been electronically mailed to:

Ryan Costello   ryan_costello@fd.org, michelle_rawson@fd.org, orx_docketing@fd.org

3:21–mj–00223–1 Notice will <u>not</u> be electronically mailed to:

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA
v.

Nickolas Sharp

ORDER SETTING CONDITIONS
OF RELEASE

Case Number: 3:21-MJ-00223-1

IT IS ORDERED that the release of the defendant is subject to the following conditions:

(1)   The defendant shall not commit any offense in violation of federal, state or local law while on release in this case.

(2)   The defendant must cooperate in the collection of a DNA sample if the collection is authorized by 42 U.S.C § 14135a.

(3)   The defendant shall immediately advise the court through Pretrial Services or defense counsel in writing of any change in address and telephone number.

(4)   The defendant shall appear at all proceedings as required and shall surrender for service of any sentence imposed as directed. The defendant shall next appear as directed by U.S. District Court.

Additional Conditions of Release

IT IS FURTHER ORDERED that the defendant be released provided that the defendant:

- Report as directed by the U.S. Pretrial Services Office.
- Do not change place of residence without the prior approval of U.S. Pretrial Services.
- Travel is limited to Oregon and the Southern District of New York for court purposes only unless prior approval is obtained from U.S. Pretrial Services.
- Surrender any passport or international travel documents to Pretrial Services or submit a statement to Pretrial Services that the defendant does not possess a passport or international travel documents. The defendant is not to apply for a new passport or international travel documents.
- The defendant shall not have direct or indirect contact with the following named persons: victim, Ubiquiti Inc.
- Not directly or indirectly use or possess a computer or electronic media, including any devices and cellular phones, with internet access capabilities or access a computer or electronic media, without the prior approval of Pretrial Services. Defendant shall also not access the internet or internet bulletin boards, or private or public computer networks without prior approval of Pretrial Services. _work laptop_
- Permit Pretrial Services to install monitoring software on any computer within the defendant's possession or control that allows random or regular monitoring of the defendant's computer use. Pretrial Services will also be allowed periodic inspection of any such computer including retrieval, copying and review of its electronic contents.
- The defendant shall not access the dark web.
- The defendant may only access and review documents provided in discover and designated as business sensitive disclose materials outside the presence of counsel, only on an electronic device with monitoring software installed and monitored by Pretrial Services.
- The defendant shall appear in the in Southern District of Florida U.S. District Court (500 Pearl Street New York, NY 10007) on **December 15, 2021 at 11am EST.**

Advice of Penalties and Sanctions

TO THE DEFENDANT:

    YOU ARE ADVISED OF THE FOLLOWING PENALTIES AND SANCTIONS:

    A violation of any of the foregoing conditions of release may result in the immediate issuance of a warrant for your arrest, a revocation of release, an order of detention, forfeiture of bond, and a prosecution for contempt of court and could result in a term of imprisonment, a fine, or both.

    The commission of any crime while on pre-trial release may result in an additional sentence to a term of imprisonment of not more than ten years, if the offense is a felony; or a term of imprisonment of not more than one year, if the offense is a misdemeanor. This sentence shall be in addition to any other sentence.

    Federal law makes it a crime punishable by up to ten years of imprisonment, and a $250,000 fine or both to intimidate or attempt to

1

intimidate a witness, victim, juror, informant or officer of the court, or to obstruct a criminal investigation. It is also a crime punishable by up to ten years of imprisonment, a $250,000 fine or both, to tamper with a witness, victim or informant, or to retaliate against a witness, victim or informant, or to threaten or attempt to do so.
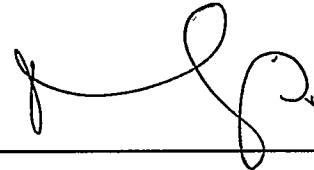
If after release, you knowingly fail to appear as required by the conditions of release, or to surrender for the service of sentence, you may be prosecuted for failing to appear or surrender and additional punishment may be imposed. If you are convicted of:

(1)   an offense punishable by death, life imprisonment, or imprisonment for a term of fifteen years or more, you shall be fined not more than $250,000 or imprisoned for no more than ten years, or both;

(2)   an offense punishable by imprisonment for a term of five years or more, but less than fifteen years, you shall be fined not more than $250,000 or imprisoned for no more than five years, or both;

(3)   any other felony, you shall be fined not more than $250,000 or imprisoned no more than two years, or both;

(4)   a misdemeanor, you shall be fined not more than $100,000 or imprisoned not more than one year, or both;

A term of imprisonment imposed for failure to appear or surrender shall be in addition to the sentence for any other offense. In addition, a failure to appear may result in the forfeiture of any bond posted.

Acknowledgment of Defendant

I acknowledge that I am the defendant in this case and that I am aware of the conditions of release. I promise to obey all conditions of release, to appear as directed, and to surrender for service of any sentence imposed. I am aware of the penalties and sanctions set forth above.

_____
Signature of Defendant

_____
City, State & Zip

Special Needs Finding:
Based upon the above conditions, including the conditions relating to:
☐   Alcohol detection
☐   Drug detection
☒   Computer monitoring
The Court is reasonably assured the defendant will appear as directed and not pose a danger to the community or any other person.

Directions to the United States Marshal
☒   The defendant is ORDERED released after processing.
☐   The defendant is ORDERED temporarily released.
☐   The United States Marshal is ORDERED to keep the defendant in custody until notified by the clerk, Pretrial Services or judicial officer that the defendant has posted bond and/or complied with all other conditions for release including space availability at a community corrections center or residential treatment facility. If still in custody, the defendant shall be produced before the duty Magistrate Judge on _____ at _____.

Date: __December 1, 2021__

HONORABLE JOHN V. ACOSTA
United States Magistrate Judge   JVA

_____
Signature of Judicial Officer
John V. Acosta
U.S. Magistrate Judge

Name and Title of Judicial Officer

cc: Defendant

2

AO 466A (Rev. 07/16) Waiver of Rule 5 & 5.1 Hearings (Complaint or Indictment)

UNITED STATES DISTRICT COURT
for the
District of Oregon

United States of America	)	
v.	)	Case No. 3:21-mj-223
Nickolas Sharp	)	
	)	Charging District's Case No. 21-CR-714
Defendant	)	

WAIVER OF RULE 5 & 5.1 HEARINGS
(Complaint or Indictment)

I understand that I have been charged in another district, the _(name of other court)_   **Southern District of New York**

I have been informed of the charges and of my rights to:

(1)   retain counsel or request the assignment of counsel if I am unable to retain counsel;

(2)   an identity hearing to determine whether I am the person named in the charges;

(3)   production of the warrant, a certified copy of the warrant, or a reliable electronic copy of either;

(4)   a preliminary hearing to determine whether there is probable cause to believe that an offense has been committed, to be held within 14 days of my first appearance if I am in custody and 21 days otherwise, unless I have been indicted beforehand.

(5)   a hearing on any motion by the government for detention;

(6)   request a transfer of the proceedings to this district under Fed. R. Crim. P. 20, to plead guilty.

I agree to waive my right(s) to:

☑   an identity hearing and production of the warrant.

☑   a preliminary hearing.

☐   a detention hearing.

☐   an identity hearing, production of the warrant, and any preliminary or detention hearing to which I may be entitled in this district. I request that any preliminary or detention hearing be held in the prosecuting district, at a time set by that court.

I consent to the issuance of an order requiring my appearance in the prosecuting district where the charges are pending against me.

Date: 12/01/2021
Defendant's signature

Signature of defendant's attorney

Ryan Costello
Printed name of defendant's attorney

AO 467 (Rev. 01/09) Order Requiring a Defendant to Appear in the District Where Charges are Pending and Transferring Bail

UNITED STATES DISTRICT COURT
for the
District of Oregon

United States of America	)	
v.	)	Case No. 3:21-mj-223
NICKOLAS SHARP	)	
	)	Charging District: Southern District of New York
Defendant	)	Charging District's Case No. 21 CRIM 714

ORDER REQUIRING A DEFENDANT TO APPEAR IN THE DISTRICT
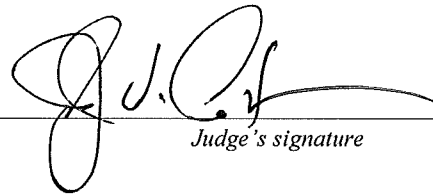## WHERE CHARGES ARE PENDING AND TRANSFERRING BAIL

After a hearing in this court, the defendant is released from custody and ordered to appear in the district court where the charges are pending to answer those charges. If the time to appear in that court has not yet been set, the defendant must appear when notified to do so. Otherwise, the time and place to appear in that court are:

Place: Daniel Patrick Moynihan United States Courthouse 500 Pearl Street New York, NY 10007-1312	Courtroom No.: Judge Katherine Failla
	Date and Time: 12/15/2021 11:00 am

The clerk is ordered to transfer any bail deposited in the registry of this court to the clerk of the court where the charges are pending.

Date: 12/01/2021

_____
Judge's signature

The Honorable John V. Acosta, U.S. Magistrate Judge
Printed name and title